UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/617,642	07/11/2003	Young Ho Park	46911/252170	5334

826 7590 11/13/2006		EXAMINER	
ALSTON & BIRD LLP		DINH, MINH	
BANK OF AMERICA PLAZA			
101 SOUTH TRYON STREET, SUITE 4000		ART UNIT	PAPER NUMBER
CHARLOTTE, NC 28280-4000		2132	

DATE MAILED: 11/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	10/617,642	PARK ET AL.
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☐ Responsive to communication(s) filed on _____.
2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-32* is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) *1-32* is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☒ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on *11 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.
   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a)☐ All   b)☐ Some * c)☐ None of:
   1.☐ Certified copies of the priority documents have been received.
   2.☐ Certified copies of the priority documents have been received in Application No. _____.
   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)
1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date *7/11/03*.
4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-32 have been examined.

Specification

2.   The disclosure is objected to because of the following informalities: "a decryptor 28 that uses a **public key** to decrypt messages coming from the physical layer of network" (page 11, lines 24-25). The specification only discloses a method and system for generating a **secret/symmetric** key for data encryption. No explanation has been given on how a public key could be used with claimed the method and system.

Appropriate correction is required.

Claim Objections

3.   Claim 20 is objected to because of the following informalities: "the combination **o** the first temporary key" (lines 2-3). Appropriate correction is required.

Claim Rejections - 35 USC § 112

4.   The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5.   Claims 12-32 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claim 12 recites the limitation "differently processing the first secret key to generate the key for data encryption in instances in which the key change information has repeated than in instances in which the key change information has not repeated" (lines 6-8). The specification first discloses that modification of the secret key generated in phase 2 is performed if it is determined that the key change information has repeated, i.e., the 8-bit size key change information space is exhausted (page 14, lines 17-25; page 17, lines 8-12). However, contradicting information is disclosed in lines 19-28 of page 17 that modification of the secret key is performed if it is determined that the key change information has not repeated. In addition, no explanation is given as to why the key needs to be modified when the key change information space is still not exhausted. Since the disclosure provides conflicting information, the disclosure fails to enable one skilled in the art to make and use the claimed invention. Claims 15, 22 and 25 are rejected on the same basis as claim 12. Claims that are not specifically addressed are rejected by virtue of their dependency.

6.   Claims 23-24 and 26 are rejected under 35 U.S.C. 112, first

paragraph, as failing to comply with the enablement requirement. Claims

23-24 and 26 are directed to a method and program for encrypting data

wherein the data, which has been WEP encrypted, is decrypted and then re-

encrypted using the claimed encryption system and method. The

specification discloses that the claimed encryption system may exist either

external to the MAC processor (i.e., between the MAC sublayer and the

physical layer as shown in figure 1) or internal to the MAC processor (page

12, lines 4-6). For claims 23-24 and 26, it is assumed that claimed

encryption system exists external to the MAC processor because there is no

reason why a packet should be encrypted, decrypted and then re-encrypted

within the same layer. Whereas the specification explains how the claimed

system encrypts a WEP encrypted packet without decrypting the packet prior

to transmission (figure 4; page 12, lines 1-4, 26-31; page 13, lines 1-7, 27-

31), the specification does not provide adequate information as to how the

claimed system decrypts the WEP encrypted packet and then re-encrypt the

packet using the claimed encryption algorithm prior to transmission.

Specifically, the specification does not disclose altering the WEB bit in the

WEB header of the WEB encrypted packet when this packet is decrypted (the

WEB bit has been previously set to indicate that the packet has been WEB

encrypted). Since the specification does not disclose WEB re-encrypting the

packet at the receiving side before the packet is transferred up the protocol

stack to the MAC sublayer, the MAC chip at the receiving side, using the

unaltered WEB bit, would automatically perform WEP decryption on the

packet even though the packet is no longer WEP encrypted. Since the

disclosure does not provide adequate information to make the

communication system works, the disclosure fails to enable one skilled in the

art to make and use the claimed invention.

7.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and
> distinctly claiming the subject matter which the applicant regards as his invention.

8.   Claims 7, 9 and 14 are rejected under 35 U.S.C. 112, second

paragraph, as being indefinite for failing to particularly point out and

distinctly claim the subject matter which applicant regards as the invention.

- Claim 7 recites the limitation "the second secret key" in lines 2-3.

  There is insufficient antecedent basis for this limitation in the claim.

  For examination purpose, the limitation is interpreted as "the

  intermediate value" (see claim 1, lines 7-8).

- Claim 9 recites the limitation "the intermediate value" (first occurrence

  at end of line 4 – beginning of line 5; second occurrence at line 6). It

  is not clear which intermediate value the limitation refers to: an

intermediate value (claim 8, lines 5-6) or a first intermediate value

(claim 9, line 4). For examination purpose, the limitation is

interpreted as "the first intermediate value".

- Claim 14 recites the limitation "wherein calculating a first secret key

  further comprises" in lines 1-2. There is insufficient antecedent basis

  for this limitation in the claim. For examination purpose, claim 11 is

  treated as being a dependent claim of claim 12 (see claim 12, line 3).

9.   Claims 1-11 are rejected under 35 U.S.C. 112, second paragraph, as

being incomplete for omitting essential steps, such omission amounting to a

gap between the steps. See MPEP § 2172.01. The specification discloses a

three-phase process to generate a key for data encryption (see figure 6 and

corresponding text). Claim 1 is directed to a method for generating a key

for data encryption; however the steps recited in the claim corresponds only

to the phase 1 of the three phases (see figure 7). The omitted steps are

the steps in phases 2-3 of the process (figures 9-11). Similarly, claim 8

recites only the steps corresponding to only phase 2, and the missing steps

are the steps in phases 1 and 3 of the process. Claims that are not

specifically addressed are rejected by virtue of their dependency.

10.   Claims 1-11 are rejected under 35 U.S.C. 112, second paragraph, as

being incomplete for omitting essential elements, such omission amounting

to a gap between the elements. See MPEP § 2172.01. The omitted element

is the key for data encryption as recited in the preamble. Both claims 1 and

8 produce a temporary key rather than a key for data encryption. Claims

that are not specifically addressed are rejected by virtue of their

dependency.

11.   Claims 12-14 are rejected under 35 U.S.C. 112, second paragraph, as

being incomplete for omitting essential elements, such omission amounting

to a gap between the elements. See MPEP § 2172.01. Claim 12 recites

"calculating a first secret key utilizing predefined key change information"

(lines 3-4). The disclosure states that the claimed invention overcomes the

drawbacks of WEP encryption algorithm such as static nature of WEP keys,

small key space, IV collisions, cross correlation between the IV and the key,

etc. (Specification, page 6, lines 6-12). However, without a MAC address

and a randomly-generated initialization vector value being used as input to

generate the secret encryption key (figures 7 and 9-10), the first secret key

generated by claim 8 would be just the same as a WEP key and would not

address the limitations of WEP encryption algorithm (specification, page 11,

lines 20-28; page 15, lines 28-31; page 16, lines 1-4; lines 15-26). Claims

that are not specifically addressed are rejected by virtue of their

dependency.

12.   Claims 12-14 are rejected under 35 U.S.C. 112, second paragraph, as

being incomplete for omitting essential steps, such omission amounting to a

gap between the steps. See MPEP § 2172.01. Claim 12 recites "calculating

a first secret key utilizing predefined key change information" (lines 3-4).

The disclosure states that the claimed invention overcomes the drawbacks of

WEP encryption algorithm such as static nature of WEP keys, small key

space, IV collisions, cross correlation between the IV and the key, etc.

(Specification, page 6, lines 6-12). However, without the steps of XORing

the MAC address with the key, hashing the XORed result, randomly

generating an IV value; XORing the hashed result and the IV value,

permuting the second XORed result as disclosed in figures 7 and 9-10, the

first secret key generated by claim 8 would be just the same as a WEP key

and would not address the limitations of WEP encryption algorithm

(specification, page 11, lines 20-28; page 15, lines 28-31; page 16, lines 1-

4; lines 15-26). Claims that are not specifically addressed are rejected by

virtue of their dependency.

Claim Rejections - 35 USC § 102

13.   The following is a quotation of the appropriate paragraphs of 35

U.S.C. 102 that form the basis for the rejections under this section made in

this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

14.   Claims 1-8, 11-12, 14-16, 18-20, 22, 25, 27 and 29-32 are rejected

under 35 U.S.C. 102(a) as being anticipated by Housley et al. ("Alternate

Temporal Key Hash"). Housley discloses a method and system for

generating an RC4 key for use with WEP (Wired Equivalent Privacy)

encryption algorithm in wireless LAN (Abstract; Section 1, Motivation).

Regarding claims 1-2, 4 and 6, Housley specifically discloses a method

for generating a key for data encryption comprising: selecting a first secret

key (TK); combining the first secret key with at least a portion of a user-

specific MAC address (TA), to result in an intermediate value (P1K);

combining the intermediate value with predefined key change information

(IV16); and transforming the combination of the intermediate value and the

predefined key change information to generate the key (RC4KEY) (Section 3,

Alternate Temporal Key Hash Function; page 12).

Regarding claim 3, Housley further discloses using a hash function (Section 3, Alternate Temporal Key Hash Function; Section 6, S-Box).

Regarding claims 5 and 7, Housley further discloses using bitwise XOR operations (Section 3, Alternate Temporal Key Hash Function).

Regarding claims 8 and 11, Housley discloses a method for generating a key for data encryption comprising: generating an Initialization Vector (IV) value (Section 5, Initialization Vector Management); combining a first secret key (TK) with the IV value (IV32) to result in an intermediate value (P1K); and permutating the intermediate value (Section 3, Alternate Temporal Key Hash Function).

Regarding claim 12, Housley discloses a method for generating a key for data encryption comprising: calculating a first secret key utilizing predefined key change information (Section 3, Alternate Temporal Key Hash Function); determining if the key change information has repeated (Section 5, Initialization Vector Management); and differently processing the first secret key to generate the key for data encryption in instances in which the key change information has repeated than in instances in which the key change information has not repeated (Section 5, Initialization Vector Management).

Regarding claim 14, Housley further discloses calculating the first secret key by selecting a predetermined secret key, combining the

predetermined secret key with a MAC address to result in a first intermediate value, combining the first intermediate value with predefined key change information and transforming the combination of the first intermediate value and the predefined key change information to result in the first secret key (Section 3, Alternate Temporal Key Hash Function; page 12).

Regarding claims 15-16, 18-20, 22, 25, 27 and 29-32, Housley discloses a method for generating a key for data encryption comprising: selecting a first secret key (TK); generating a first temporary key (P1K) based upon a combination of the first secret key with a MAC address (TA) and further based upon predefined key change information (IV counter); generating a second temporary key (RC4KEY) based upon a combination of the first temporary key and an IV value (IV counter) (Section 3, Alternate Temporal Key Hash Function); determine if the predefined key change information has repeated; setting the second temporary key to be the final key for data encryption if the predefined key change information has not repeated; encrypting data to be transmitted with the final key (Section 5, Initialization Vector Management).

15.   Claim 8 is rejected under 35 U.S.C. 102(b) as being anticipated by "ANSI/IEEE Std 802.11 - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" (hereinafter "802.11

Standard"). "802.11 Standard" discloses a method for generating a key

sequence for WEP encryption algorithm comprising: generating an IV value;

combining a first secret key with the IV value to result in an intermediate

value, i.e., seed; and permutating the intermediate value to generate the

key sequence (Section 8.2.3, WEP theory of operation, page 63).

Claim Rejections - 35 USC § 103

16.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis

for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or
> described as set forth in section 102 of this title, if the differences between the subject
> matter sought to be patented and the prior art are such that the subject matter as a
> whole would have been obvious at the time the invention was made to a person having
> ordinary skill in the art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

17.   Claims 9-10 and 21 are rejected under 35 U.S.C. 103(a) as being

unpatentable over "802.11 Standard" as applied to claim 8 above, and

further in view of Housley.

Regarding claim 9, "802.11 Standard" only discloses generating a key

sequence from the first secret key. 802.11 Standard does not disclose

generating the first secret key. Housley discloses a method for generating a

key secret key by selecting a predetermined secret key, combining the

predetermined secret key with a MAC address to result in a first intermediate

value, combining the first intermediate value with predefined key change

information and transforming the combination of the first intermediate value

and the predefined key change information to result in the first secret key

(Section 3, Alternate Temporal Key Hash Function; page 12). It would have

been obvious to one of ordinary in the art at the time the invention was

made to incorporate the Housley method for generating a secret key into the

method of generating a key sequence from a secret key disclosed by

"802.11 Standard". The motivation for doing so would have been to

improve security of WEP encryption algorithm (Section 1, Motivation).

Regarding claims 10 and 21, "802.11 Standard" does not disclose

generating the seed using the MAC address. Housley discloses generating a

seed using the sender's MAC address (Section 2, Introduction). It would

have been obvious to one of ordinary in the art at the time the invention was

made to modify the method in "802.11 Standard" to use a MAC address in

generating a seed, as disclosed by Housley. The motivation for doing so

would have been to ensure that various parties encrypting with the same

secret key use different key stream (Section 2, Introduction).

"802.11 Standard" does not disclose using a timer value in generating

an initialization vector. Official Notice is taken that both the concept and

advantage of using a timer value such as a timestamp in generating an

initialization vector are well known and expected in the art because of its

random nature. It would have been obvious to one of ordinary in the art at

the time the invention was made to use a timestamp in generating an

initialization vector because of its random nature.

18.   Claims 13, 17 and 28 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Housley as applied to claims 12, 15 and 25 above, and

further in view of Kelem et al. (6,118,869). Housley does not disclose

processing the first secret key comprises performing a bitwise shift of the

first secret key in instances in which the key change information has not

repeated. Kelem discloses an encryption method comprising performing a

bitwise shift of a secret key in instances in which the key change information

has not repeated (Abstract; col. 2, lines 1-9, 56-65; col. 4, lines 8-38). It

would have been obvious to one of ordinary in the art at the time the

invention was made to modify the Housley method to perform a bitwise shift

of a secret key in instances in which the key change information has not

repeated, as disclosed by Kelem. The motivation for doing so would have

been to provide a high level of security in an encrypted bitstream.

19.   Claims 23-24 and 26 are not rejected over the prior art.

Conclusion

20. The prior art made of record and not relied upon is considered

pertinent to applicant's disclosure.

U.S. Patent No. 6,931,132 to Billhartz et al.

U.S. Patent App. Publication No. 2006/0078124 to Whelan et al.

Walker, J., "Unsafe at any key size; An analysis of the WEP

encapsulation"

Any inquiry concerning this communication or earlier communications

from the examiner should be directed to Minh Dinh whose telephone number

is 571-272-3802. The examiner can normally be reached on Mon-Fri:

10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the

examiner's supervisor, Gilberto Barron can be reached on 571-272-3799.

The fax phone number for the organization where this application or
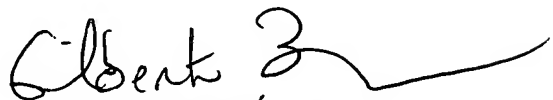
proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained

from the Patent Application Information Retrieval (PAIR) system. Status

information for published applications may be obtained from either Private

PAIR or Public PAIR. Status information for unpublished applications is

available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on

access to the Private PAIR system, contact the Electronic Business Center

(EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-

1000.

MP

Minh Dinh
Examiner
Art Unit 2132

MD
11/06/06

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100